The Use of Fault Trees for the Design of Robots for Hazardous Environments

Ian D. Walker • Rice University • Houston

Joseph R. Cavallaro • Rice University • Houston

Key Words: Fault Trees, Robotics, Interval Data.

SUMMARY & CONCLUSIONS

This paper addresses the application of fault trees to the analysis of robot manipulator reliability and fault tolerance. Although a common and useful tool in other applications, fault trees have only recently been applied to robots. In addition, most of the fault tree analyses in robotics have focused on qualitative, rather than quantitative, analysis. Robotic manipulators present some special problems, due to the complex and strongly coupled nature of their subsystems, and also their wild response to subsystem failures. Additionally, there is a lack of reliability data for robots and their subsystems. There has traditionally been little emphasis on fault tolerance in the design of industrial robots, and data regarding operational robot failures is relatively scarce.

However, at this time there is a new and critical need for safe and reliable robots for remote Environmental Restoration and Waste Management applications. The question of how to best incorporate fault tolerance and reliability into the design of such remote manipulators remains an open issue, and is the subject of current research. This paper discusses aspects of the reliability problem in robotics, concentrating on the quantitative aspects of fault tree analysis for the design of robot manipulators.

1. INTRODUCTION

In spite of the fact that robotics has been a rapidly developing area in the last few years, there has been relatively little work in robot reliability and fault tolerance until recently [15]. Robot manipulators are a critical mix of mechanical, electrical, and electronic components. Consequently, there are numerous critical failure modes inherent in a typical manipulator system. The situation is compounded by the fact that robot systems are highly dynamic, resulting in very rapid and wild responses of robots to subsystem failures. Due to the dynamic and nonlinear nature of robots, much reliability analysis is necessarily complex and often both configuration and trajectory dependent.

Robots are being increasingly deployed in remote and hazardous environments, which make reliability and fault tolerance of even more critical importance than previously. Some key research in robot reliability is already under way [8, 11, 15]. This paper discusses the particular concerns involved in the synthesis and analysis of fault trees for robotics applications. Fault trees have only recently been applied to robots [5, 7, 14], where much of the work has been for qualitative analysis [15]. Our work is focused on remote manipulators for remediation of highly radioactive waste. This application presents special problems, as discussed in the following section.

1.1 Notation List

Ji	Robot Joint i
Si	Robot Sensor i, Optical Encoder
Mi	Robot Actuator i, Electric Motor
λ	Component Failure Rate
t	Mission Time
p	Component Failure Probability
p_{ll}, p_l, p_r, p_{rr}	Component Failure Probability Interval Points

0-7803-3112-5/96/$5.00 © 1996 IEEE

2. ROBOTICS FOR ENVIRONMENTAL RESTORATION

Robotic arms will be deployed to assist in remediation of the waste tanks at the Hanford, Washington, Nuclear Site. At Hanford, about $140,000m^3$ of high-level radioactive waste is being stored in 149 single-shell tanks (SSTs) [10]. This waste has been produced at Hanford since the 1940's as a by-product of processing spent nuclear fuel for uranium and plutonium recovery.

The U.S. Department of Energy (DOE) has established a program to remove, treat, and dispose of the wastes stored in these underground tanks. The goal is to 'develop and field retrieval systems with the capability to remove wastes from these tanks and transfer those wastes for further downstream processing' [10]. Long reach manipulators are the technology selected by DOE to remove the waste from the tanks.

In earlier work [17], we have developed fault trees to support the design of an underground storage tank manipulator for Environmental Restoration and Waste Management [2]. The robot is to be deployed in single-shell underground storage tanks at the DOE site in Hanford, Washington. The manipulator is to be lowered into the tank from above, and is required to move within the tank and remove or remediate waste in the tank as shown in Fig. 1. The proposed robot will be required to maneuver around various pipes and debris within the underground storage tank. The waste removal end effector will need to be carefully positioned above the waste to quickly and effectively remove as much waste as possible. The robot will be kinematically redundant (have more than six joints) so that the manipulator will have sufficient dexterity to avoid obstacles.

Reliability and fault tolerance are clearly of prime importance in this application. The manipulator must "fail safe" within the tank, to prevent possible spillage of the waste into the environment. In addition, in the event of a failure in the robot system, the arm must be removable from the tank. These requirements impose significant design restrictions on the arm. Reliability is a key issue in the design phase, and our work in fault tree analysis is in support of the early design phase for the manipulator. Our fault trees include failure modes from the mechanical, sensor, and computer control subsystems as well as the human operator [17].

A standard qualitative analysis of the fault trees was useful, and resulted in a series of recommended changes to the original manipulator design [17]. It is to be expected that a quantitative analysis will provide significant further insights. However, quantitative reliability analyses of the fault trees is more problematic in the robotics application, due in part to uncertain data and repeated events in the trees. The following sections discuss these issues in more detail.

3. FAULT TREE ANALYSIS FOR ROBOTS

In this section, for the purpose of illustration, we first discuss a two-joint planar robot, with one position sensor and actuator at each joint. This robot represents a two joint subset of the original design for the waste retrieval arm considered in [17], and will be used here for demonstration purposes. A fault tree for a general manipulator would of course be much more detailed, but this basic example will serve to demonstrate many of the key issues in robot fault tree analysis. From a reliability point of view, the robot represented by Figure 2 is the least favorable design, since two joints are the minimum possible for arbitrary positioning in a planar workspace, and a failure in either sensor or actuator will typically lead to a wild failure response [15]. With only a single sensor or actuator per joint, the control algorithm is vulnerable to errors and may incorrectly move the robot arm if a failure occurs. This basic robot failure scenario will be studied in the fault trees in this paper. Figure 2 shows a fault tree for the two joint robot in the plane where **M 1** refers to the actuator (motor) on joint one, **J 1**. There is only a single sensor **S 1** at this joint. The second joint is similarly labeled. The trees have been evaluated using the FaultrEASE software package [19].

From Figure 2, it can be observed that the failure of any motor or sensor will lead to robot failure. In order to improve the fault tolerance of the robot system, a glance at the fault tree reveals several modifications that can be made to the robot. Perhaps, the simplest improvement is to add a redundant sensor at each joint. This is indicated by the AND gate with sensors **S 1A** and **S 1B** at **J 1** in Figure 3. It is technically more difficult to add additional motors to drive a joint of a robot. One possible solution is to add entire additional joint assemblies, so that a three joint robot in the plane could gracefully degrade to a two joint robot in the presence of a fault in one of the

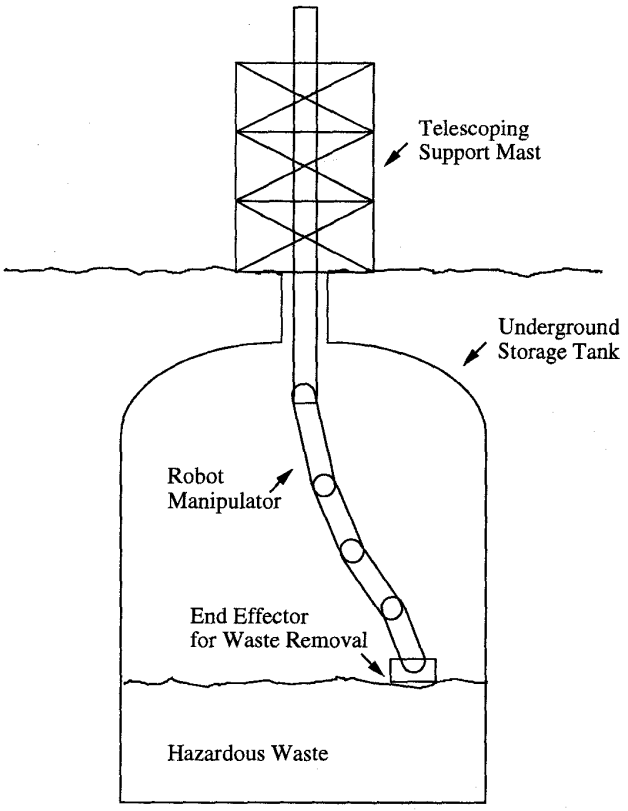

Figure 1: Design concept for hazardous waste retrieval robot.

motors. It is assumed that it will be possible to lock the failed joint and that the robot planning task can be modified to compensate for the reconfiguration. Therefore, two of the three joints shown in the fault tree in Figure 3 must fail before there is robot operational (top event) failure. The fault tree has been drawn explicitly to show the pairings of the robot joints. There are 12 cutsets in this fault tree. For example, the primary events **M 1**, **S 2A**, and **S 2B** form a cutset. The various sensors and motors now appear as repeated events within the fault tree. This tree structure and modification is typical of the type of results obtained in qualitative analysis of more detailed robot fault trees [17]. In the following section, quantitative aspects of the analysis of these trees will be presented to illustrate the issues and difficulties inherent in the case of the more detailed robot fault trees.

4. QUANTITATIVE ISSUES

For some robot subsystems, standard techniques [13] can be used to analyze their reliability through fault trees. However, a key difficulty for quantitative reliability analysis of robots is that reliability data for important subsystems and components is not well established or trusted. This is particularly true for robots to be deployed in hazardous and radioactive environments [15]. In many cases, reliability data for robot components in these environments is at best approximately known. Thus, in order to quantitatively analyze the overall fault trees, some type of approximate analysis, which combines conventional reliability analyses for well understood subsystems with reliability estimates for less well understood subsystems, is required.

One useful type of approximate analysis is based on the technique of interval analysis [6] where ranges of numbers are systematically combined. Range failure information is an attractive option in the case of uncertain data, and may be readily derived from existing data. For example, failure rate data for non-radioactive environments [1] can be expanded into a failure rate interval to study the reliability of robots used in hazardous radioactive environments. This ap-

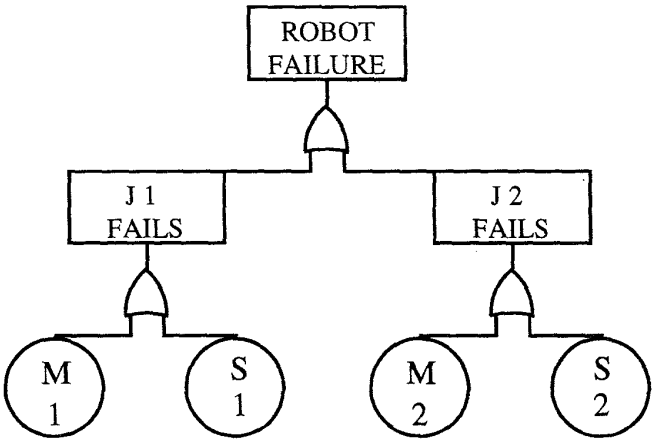

Figure 2: Fault Tree for a basic two joint planar robot.

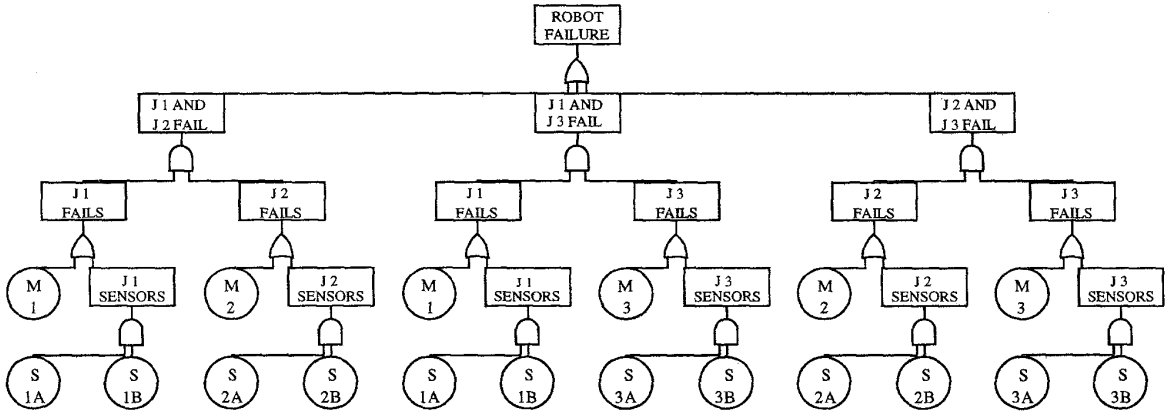

Figure 3: Fault Tree for a redundant three joint robot with multiple sensors.

proach, which allows for "approximate", or "fuzzy" failure probabilities, is strongly related to fuzzy logic techniques [4, 12, 18] for dealing with uncertainty in the data. We will next use the fault trees from the previous section to outline one such approach, which is based on manipulating (based on subsystem reliability estimates and the structure of the fault trees) approximate ranges of subsystem reliabilities.

Table 1 shows reliability interval data that is derived from the 1995 Nonelectronic Parts Reliability Data (NPRD-95) failure rate tables [1]. It was observed in NPRD-95 that 68 percent of failure rates will be between 0.22 and 4.5 times the reported value. Furthermore, 90 percent of failure rates were between 0.8 and 11.9 times the reported value. The total mission operation time for the robot to operate in a single underground storage tank would be on the order of 1,000 hours. The robot would then be carefully decontaminated and removed from the tank. Maintenance would be performed and then the robot would be moved to the next tank at the Hanford site to continue waste removal. In this case, an approximate probability of failure [13] was determined as λt, where $t = 1000$ hours. Since the robot will be used in a hazardous radiation environment which is beyond the scope of NPRD-95, the failure probability was expanded over an interval. The given failure probability p is expanded into an inner interval $[p_l, p_r]$ such that $p_l = 0.8p$ and $p_r = 4.5p$ and an outer interval $[p_{ll}, p_{rr}]$ such that $p_{ll} = 0.22p$ and $p_{rr} = 11.9p$. The four point interval based on the NPRD-95 ranges is shown in Figure 4. Using these estimates, Table 1 shows the interval data to be used in the fault tree analysis. For the electric motor the base failure probability from NPRD-95 is $p = 0.00924$ and for the optical encoder sensor the failure probability is $p = 0.0155$.

For the basic two joint robot described in Figure 2, the following probabilities shown in Table 2

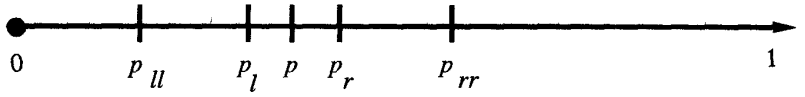

Figure 4: Failure probability interval.

Table 1: Reliability Estimates for Redundant Planar Robot Components.

Component	p_{ll}	p_l	p_r	p_{rr}
Electric Motor	0.000739	0.00203	0.0416	0.11
Optical Encoder Sensor	0.00124	0.00341	0.0698	0.184

were calculated for the top event. These inner and outer component failure probability intervals are numerically propagated through the fault tree to produce intervals for the top level failure event. This approach is similar to the fuzzy analysis in [12]. The exact probability of failure is $p = 0.0490$ in this case.

A similar quantitative analysis can be performed for the three joint redundant planar robot shown in Figure 3. This configuration shows a reduction in failure probability due to the additional sensors and joint. The exact probability of failure of the top event is $p = 0.000268$.

The robot fault tree discussed above for the fault tolerant robot displays repeated events at the sensor level, leading to added complexity in a quantitative analysis [9]. From this analysis, the probability of robot operational failure has been reduced from $p = 0.0490$ to $p = 0.000268$. This represents an improvement of approximately a factor of 200 for the redundant fault tolerant design for the mission time of 1,000 hours. It is also interesting to note that the worst case outer failure probability interval point for the three joint redundant robot, $p_{rr} = 0.0534$ fits within the inner failure probability interval, $[p_l, p_r] = [0.0109, 0.223]$ for the basic non-fault tolerant two joint planar robot design. This data shows that the additional complexity in adding redundant sensors and joints yields tangible reliability improvements. The quantitative analysis backs up the intuitive qualitative analysis surrounding the initial discussion of the fault trees. With multiple sensors present, it becomes important to have efficient fault detection algorithms to make use of this redundancy.

5. APPLICABILITY AND FUTURE WORK

The potential for successful application of fault trees in robotics extends well beyond the design phase discussed in this paper. One proposed approach for the use of fault trees as a framework for real-time robot fault tolerance software is discussed in [14]. A critical issue here is that of including fault detection and coverage in the analysis. The timescale for the occurrence of robot faults is typically on the order of many hours, where undetected and/or uncovered faults typically critically affect the system in the order of milliseconds. Thus techniques which combine the concise representation of fault trees with efficient coverage models will be important in the future.

The approach suggested in [3], which decomposes fault occurrence and fault recovery into two separate submodels, appears to be have significant potential for robotics. The approach, which combines fault tree and coverage models efficiently, could be directly applicable for those subsystems of the robot (control computer, etc.) whose coverage models can be consistently defined independent of the robot configuration or task.

One critical complication with robot manipulators is that other fault detection models, for example for those subsystems in motion within the arm (sensors, actuators, etc) will be configuration-dependent, i.e. vary with each manipulator motion trajectory. This means that coverage models must be augmented with trajectory dependent information. For example, consider fault detection for a robot wrist joint position sensor. For the manipulator performing a "pick and place" task, it is mostly the shoulder and elbow (proximal) joints that are used for gross positioning. In this case, the wrist (distal) joints are moved very

Table 2: Reliability Estimates for Basic Two Joint Planar Robot Failure.

	p_{ll}	p_l	p_r	p_{rr}
Robot Failure	0.00396	0.0109	0.223	0.588

Table 3: Reliability Estimates for Redundant Planar Robot Failure.

	p_{ll}	p_l	p_r	p_{rr}
Robot Failure	0.00000164	0.0000125	0.00622	0.0534

sparingly, if at all. Thus, the wrist sensor readings are largely isolated from effects from the remainder of the arm, and spurious wrist sensor readings (perhaps from a terminal sensor fault) will be relatively easy to distinguish and isolate. However, in the case of rapid fine motions (largely involving the wrist joints), dynamic coupling between the wrist joints can introduce significant errors in the controller, which enter the sensor readings as extra noise [16]. In this case fault detection becomes a much more complex problem [16], the coverage model takes a different form, and probabilities are significantly altered.

This simple example motivates the need for more dynamic coverage models than are in operation at the present time. Most fault detection methods currently employed in robots are quite ad hoc, and are based on comparing sensor readings with expected other sensed values, and masking normal sensor errors with fixed thresholds. These thresholds are determined empirically for specific trajectories. The imprecision in this approach has led to both false alarms and missed faults [15]. Algorithms for robot fault detection which theoretically guarantee complete detection and coverage for robot arms under certain assumptions have been established and analyzed recently [16]. However, much more work needs to be done in the area of robot coverage models in order to draw general conclusions regarding robot fault coverage.

In conclusion, we have found that fault trees are an excellent technique for analyzing reliability and fault tolerance in a multidisciplinary area such as robotics. Qualitative fault tree analyses have proved valuable for various robotic applications [5, 7, 15, 17]. Quantitative analyses for robotics are more problematic due to the limited data on these custom systems. However, such estimates are important in the manipulator design process, and the techniques discussed in this paper offer a systematic technique for quantitative analysis of reliability and fault tolerance for robots.

6. ACKNOWLEDGMENTS

This work was supported in part by the National Science Foundation under grants IRI-9526363 and DDM-9202639, by DOE Sandia National Laboratory Contract AL-3017, by DOE contract DE-AC04-94AL8500, and by NASA contract NAG-9-740. The authors would also like to thank Jason Kincaid for developing the numerical examples.

REFERENCES

[1] W. Denson, G. Chandler, W. Crowell, A. Clark, and P. Jaworski. Nonelectronic Parts Reliability Data. Technical Report NPRD-95, Reliability Analysis Center, Rome, NY, July 1994.

[2] Department of Energy, Washington, D.C. *Environmental Restoration and Waste Management 5-Year Plan, Fiscal Years 1994-1998*, January 1993. DOE/S-00097P, Vol. 1-2.

[3] S.A. Doyle and J. Bechta Dugan. Fault trees and Imperfect Coverage: A Combinatorial Approach. In *Proceedings of the IEEE Reliability and Maintainability Symposium*, pages 214–219, Atlanta, GA, January 1993.

[4] J.A.B. Geymayr and N.F.F. Ebecken. Fault Tree Analysis: A Knowledge-Engineering Approach. In *Proceedings of the IEEE Reliability and Maintainability Symposium*, pages 37–45, Washington, D.C., January 1995.

[5] V. H. Guthrie and D. K. Whittle. RAM Analysis Software for Optimization of Servomanipulator

Designs. DOE SMALL BUSINESS INNOVATIVE RESEARCH (SBIR) PROGRAM REPORT JBFA-101-89, JBF Associates, Inc., Knoxville, TN, March 1989. Performed for Oak Ridge National Laboratory.

[6] R.E. Moore. *Interval Analysis.* Prentice-Hall, Englewood Cliff, NJ, 1966.

[7] NASA. Computer Based Control System Noncompliance Report for Computer Independent Hazard Control System. REPORT, NASA Goddard Flight Center, Greenbelt, MD, September 1991.

[8] C.A. Ntuen and E.H. Park. A Formal Method to Characterize Robot Reliability. In *Proceedings of the IEEE Reliability and Maintainability Symposium,* pages 395–397, Atlanta, GA, January 1993.

[9] S. Rai. A Direct Approach to Obtain Tighter Bounds for Large Fault Trees with Repeated Events. In *Proceedings of the IEEE Reliability and Maintainability Symposium,* pages 475–480, Anaheim, CA, January 1994.

[10] E.J. Shen. Retrieval of Underground Storage Tank Wastes: The Hanford Challenge. In *Proceedings of the American Nuclear Society Topical Meeting on Robotics and Remote Systems,* pages 549–553, Monterey, CA, 1995.

[11] Z. Shi. Reliability Analysis and Synthesis of Robot Manipulators. In *Proceedings of the IEEE Reliability and Maintainability Symposium,* pages 201–205, Anaheim, CA, January 1994.

[12] H. Tanaka, L.T. Fan, F.S. Lai, and K. Toguchi. Fault Tree Analysis for Fuzzy Probability. *IEEE Transactions on Reliability,* R-32(5):453–457, December 1983.

[13] W. E. Vesley, F. F. Goldberg, N. H. Roberts, and D. F. Haasi. Fault Tree Handbook. NUREG 0492, Systems and Reliability Research Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission, Washington DC, January 1981.

[14] M. L. Visinsky, J. R. Cavallaro, and I. D. Walker. Expert System Framework of Fault Detection and Fault Tolerance in Robotics. *International Journal of Computers and Electrical Engineering,* 20(5):421–435, 1994.

[15] M. L. Visinsky, J. R. Cavallaro, and I. D. Walker. Robotic Fault Detection and Fault Tolerance: A Survey. *Reliability Engineering and System Safety,* 46(2):139–158, 1994.

[16] M. L. Visinsky, J. R. Cavallaro, and I. D. Walker. A Dynamic Fault Tolerance Framework for Remote Robots. *IEEE Transactions on Robotics and Automation,* 1995. to appear.

[17] I. D. Walker and J. R. Cavallaro. Failure Mode Analyses of the Hanford Manipulator. Technical Report TR-9402, Dept. of Electrical and Computer Engineering, Rice University, Houston, TX, March 1994.

[18] D.P. Weber. Fuzzy Weibull for Risk Analysis. In *Proceedings of the IEEE Reliability and Maintainability Symposium,* pages 456–461, Anaheim, CA, January 1994.

[19] G. C. Wilcox. FaultrEASE User's Manual. Technical report, Arthur D. Little, Inc., Cambridge, MA, 1992.

BIOGRAPHIES

Ian D. Walker, *PhD*
Department of Electrical and Computer Engineering
Rice University
Houston, Texas 77251-1892 USA
Internet (e-mail): ianw@rice.edu

Ian D. Walker received the B.Sc. degree in Mathematics from the University of Hull, England, in 1983. He received the M.S. degree in 1985, and the Ph.D. in 1989, both in Electrical Engineering, from the University of Texas at Austin. In 1989 he joined the faculty of Rice University, Houston, TX, where he is an Associate Professor of Electrical and Computer Engineering. His research interests are in the areas of robotics and control, particularly fault tolerant robot systems; robotic hands and grasping; and kinematically redundant robots.

Joseph R. Cavallaro, *PhD*
Department of Electrical and Computer Engineering
Rice University
Houston, Texas 77251-1892 USA
Internet (e-mail): cavallar@rice.edu

Joseph R. Cavallaro received the B.S. degree from the University of Pennsylvania, Philadelphia, PA, in 1981, the M.S. degree from Princeton University, Princeton, NJ, in 1982, and the Ph.D. degree from Cornell University, Ithaca, NY, in 1988, all in electrical engineering. From 1981 to 1983, he was with AT&T Bell Laboratories, Holmdel, NJ. In 1988 he joined the faculty of Rice University, Houston, TX, where he is an Associate Professor of Electrical and Computer Engineering. His research interests include computer arithmetic, fault tolerance, VLSI design and microlithography, and VLSI architectures and algorithms for parallel processing and robotics.